Schrems II Re-Examined

Christopher Kuner 2020-08-25T09:35:02

The Court of Justice of the EU's judgment in *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems* ("*Schrems II";* case C-311/18) of 16 July has already received significant attention. Now that the dust has somewhat settled, however, it deserves re-examination in light of its significant implications for the regulation of international data transfers under the EU General Data Protection Regulation ("GDPR"). In this contribution I will explore four important issues that *Schrems II* raises under the GDPR, namely (1) that the judgment makes significant changes to some long-held assumptions about how data transfers are regulated under the GDPR; (2) that the Court's approach to the use of the Commission-approved standard contractual clauses (SCCs) for the transfer of personal data is somewhat tautological; (3) that the Court may not have put data transfers to the US in as much immediate danger as many commentators seem to assume; and (4) that the judgment may weaken the attractiveness of the GDPR as a model for other countries to adopt.

The GDPR's framework for data transfers

In *Schrems II* the Court seemed to ignore the hierarchical structure of data transfer mechanisms on which Chapter V GDPR is based, and thus to throw in question long-established assumptions about the relationship between them.

The data protection authorities (DPAs) have traditionally required that the data exporter first consider whether the third country provides an adequate level of protection under Article 45 GDPR (i.e., whether an adequacy decision has been issued for the country of transfer), and then provide adequate safeguards under Article 46 if an adequacy decision is not available (see Guidelines 2/2018 of the European Data Protection Board (EDPB), pp. 3-4). This puts adequacy decisions at the top of the hierarchy, with appropriate safeguards being available if one cannot be used. The hierarchical relationship between the two follows both from the language of Article 46(1) GDPR, and from the fact that an adequacy decision is based on a deeper and broader investigation of a third country's entire legal system than is possible for parties using adequate safeguards for individual data transfers.

However, in *Schrems II* the Court held not only that the standard of "essential equivalence" with EU law applies to adequate safeguards such as the SCCs (para. 96), but that the criteria for assessing adequacy contained in Article 45(2) do as well (para. 104). The Court thus abandoned the hierarchy between these two data transfer mechanisms, despite the express language of the GDPR and the long-standing practice of the DPAs. One could even ask what point there is of the Commission assessing third countries for adequacy if appropriate safeguards based on the same standards are available, in light of the fact that they can be implemented much more quickly than an adequacy decision can be approved.

In the hierarchy of data protection mechanisms, the derogations under Article 49 GDPR rank at the bottom, since they are not designed to provide protection and are to be used only when an adequacy decision or appropriate safeguards are not available (Article 49(1)). The Court makes a cryptic reference to the derogations in para. 202, stating that "in view of Article 49", invalidation of the Commission's decision approving the Privacy Shield as adequate does not create a legal vacuum. This seems to imply that use of the derogations can help compensate for invalidation of the Privacy Shield. However, both the wording of Article 49 and the position of the EDPB (EDPB Guidelines 2/2018, p. 4) make it clear that the derogations are to be strictly interpreted, as follows from the Court's own holdings that derogations from fundamental rights are to be used only when strictly necessary (see Case C-362/14 *Schrems*, para. 92). Thus, the derogations cannot fill the gap created by invalidation of the Privacy Shield, except in a few limited cases.

The Court and the standard contractual clauses

Prior to *Schrems II* there was much anxiety about whether the Court would invalidate the SCCs on the basis that they are concluded between parties transferring personal data and cannot bind third country authorities. The Court upheld use of the SCCs approved in Commission Decision 2010/87/EU and amended in Commission Implementing Decision 2016/2297, finding that the protections they provide rest not on the legal system of the third country of transfer (as with an adequacy decision), but on protections that the parties transferring the data provide to ensure an adequate level of protection (para. 131), which may include supplementary measures such as "other clauses or additional safeguards" (para. 132). However, the Court's reasoning here seems tautological, i.e., it held that while contractual clauses cannot bind third country authorities this can be remedied though safeguards including additional clauses (para. 132).

A more convincing argument for upholding the SCCs is the Court's positive evaluation of the various provisions in them that allow transfers to be suspended or prohibited when the clauses are breached or it becomes impossible to honour them (paras. 137-148), and the emphasis it puts on them providing "effective mechanisms" (para. 147). Having helped negotiate the 2010 SCCs with the Commission on behalf of the International Chamber of Commerce (see FN 4 to Recital 7 of Commission Decision 2010/87/EU), I am pleased that the Court upheld the protections they contain; indeed, to my knowledge this is the only time the Court has given a positive endorsement to any data transfer mechanism.

The Court did not specify the content of other clauses or additional safeguards that parties may use with the SCCs, but, as discussed above, they will have to take into account the conditions for adequacy contained in Article 45(2)(a). Placing evaluation of criteria for adequacy in the hands of parties that carry out data transfers may lead to legal uncertainty, as the Court recognized (para. 147). The EDPB has stated that it will provide further guidance in this regard (EDPB FAQs of 23 July 2020, p. 5), but settling disputes under Article 65 GDPR between the DPAs on the types of safeguards to be used could require the EDPB to opine on issues that could be

politically explosive, such as whether particular third countries abide by the rule of law or respect fundamental rights.

It is important to note that the Court does not require that additional safeguards provide a 100% guarantee that access to data by third parties can never occur, but rather that they constitute “effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection required by EU law…” (para. 137). Thus, they should be evaluated under a standard of proportionality, not of perfection. A few examples of clauses and safeguards could include the following:

- **Legal measures:** The parties to the transfer could agree on enhanced legal guarantees that build on those in the SCCs but provide stricter conditions for suspending data flows and deleting data in cases of unauthorized government access, as well as stricter penalties for breaches of their obligations.
- **Technical measures:** Strong encryption could be used to make it nearly impossible for unauthorized actors to read the data.
- **Organisational measures:** Groups of data exporters and importers (such as in a trade association) could commit to suspend data transfers to countries that do not respect the rule of law, based on internationally-recognized standards (for example, those published by the World Justice Project). This approach is already used in other areas, such as fair labour standards.

Data transfers to the US

Since the judgment was announced, there have been apocalyptic predictions about how it may mean the end of data transfers to the US. However, the reality will probably be less dramatic. While numerous complaints have already been filed (including by noyb, the NGO headed by Schrems), the wheels of data protection enforcement turn slowly, in particular since pan-European complaints (i.e., those that involve data transfers from multiple Member States) have to go through the EDPB, which has become infamous for delays. The DPAs also tend to be careful not to issue high-profile penalties before being completely sure that they have a strong legal case. This means that data will likely continue to flow over the Atlantic for some time before the GDPR enforcement machinery really starts to bite.

Two of the main issues the Court focused on in invalidating the Privacy Shield were the Ombudsman mechanism and data access by US authorities. The issues surrounding the Ombudsman may be the easier of the two to deal with in a legal sense (assuming the political will to do so in the US), and a thoughtful proposal in this regard has been made by Ken Propp and Peter Swire.

The issue of government data access is more difficult, as it will require strict adherence to the proportionality criteria that the Court set out (see para. 176 et seq). In this regard, a close examination of the Court’s *Opinion 1/15*, where it invalidated a proposed international agreement with Canada because of data protection concerns, could provide a useful starting point. Further guidance from the Court may be forthcoming soon in joined cases C-623/17, C-511/18, C-512/18 and C-520/18, which involve a challenge to data collection for national security

and counter-terrorism purposes in various Member States plus the UK. If, as can probably be expected, the judgments in these cases result in the Court restricting data processing for these purposes, it may help identify measures that could put EU-US data flows on a firmer legal footing.

With the Court taking such a strict position in *Schrems II*, any hope of a stable and viable accommodation for data transfers between the EU and the US can only be based on changes to US law. This will depend on political factors that are impossible to predict, and in particular on the results of the forthcoming US elections.

Implications for the global reach of the GDPR

The EU has positioned the GDPR as the global reference point for data protection and privacy (see, for example, the joint statement in May 2020 by Commissioners Jourová and Reynders). Numerous countries have sought EU adequacy decisions or adopted data protection legislation based on the EU model, and the GDPR has been a success story in this regard.

Promoting the GDPR in other regions with different legal and cultural traditions requires the EU to walk a fine line: the standard of protection should be high in order to make it a desirable model, but it must be set at a level that is possible for third countries to attain. Striking the right balance is made more difficult by the apparent tension between the Court, which has tightened the legal standards for data transfers in recent years, and the Commission, which almost seemed to welcome the invalidation of the Privacy Shield as an opportunity to negotiate a yet another data transfer agreement with the US (see the statement of Commissioner Reynders following the judgment).

However, the judgment may cause some third countries to question whether it is worthwhile to strive to reach the EU's data protection standards and to engage in protracted negotiations only to have the agreement, or the adequacy decision based on it, invalidated later on. Having now ensured that data transfers must meet a high standard, the EU should also take care not to set the bar too high, or it may make the GDPR a less attractive model for third countries.
